



GDPR:n vaikutukset käyttäjien seurannan toteuttamiseen evästeillä

Oulun yliopisto
Tieto- ja sähkötekniikan tiedekunta
Tietojenkäsittelytieteet
LuK-tutkimus
Jukka Hyytiälä
2021

Tiivistelmä

Tässä työssä tutkittiin kirjallisuuskatsauksen muodossa, miten GDPR on vaikuttanut käyttäjien seurannan toteuttamiseen evästeillä. GDPR on vaikuttanut internetsivuihin kevästä 2018 lähtien, joten aiheesta löytyi tutkimusta lähinnä vuodesta 2019 lähtien.

Tutkimuksessa havaittiin, että käyttäjien seurannan toteuttaminen on muuttunut GDPR:n käyttöönoton jälkeen, mutta se ei ole vähentynyt merkittävästi. Muutokset ovat kohdistuneet lähinnä evästekyselyihin.

Tutkimuksessa havaittiin myös, että aiheetta on tutkittu enimmäkseen lain kirjaimen noudattamisen näkökulmasta. Uusimmissa tutkimuksissa on kuitenkin tutkittu myös asiaan liittyviä seurannaisvaikutuksia, ja näin ollen tutkimuksen näkökulma näyttäisi olevan siirtymässä siihen, mitä hyötyä hyvästä tietosuojasta voisi olla.

Avainsanat

GDPR, tietosuoja, käyttäjien seuranta, evästeet, seurantaevästeet, kolmannen osapuolen evästeet

Ohjaaja

Tohtori, dosentti Raija Halonen

Sisälllys

Tiivistelmä.....	2
Sisälllys	3
1. Johdanto.....	4
2. Tutkimusmenetelmä	6
3. Tutkimustulokset	7
3.1 Evästeistä kertominen	7
3.2 Erilaiset evästekyselyt.....	8
3.3 Evästeistä kieltäytyminen	9
3.4 Kolmannen osapuolen evästeet	11
3.5 Valmiskyselyt.....	12
3.6 Lopuksi.....	13
4. Pohdinta	14
4.1 Lain kirjaimen noudattaminen	14
4.2 Kolmansien osapuolien harjoittama seuranta	15
4.3 Evästekyselyiden käytön vaikutukset	15
4.4 Käyttäjien seurannan tulevaisuus.....	15
5. Johtopäätökset	17
Lähteluettelo	18

1. Johdanto

Vuonna 2018 Euroopan unionin alueella otettiin käyttöön yleinen tietosuoja-asetus GDPR (Euroopan unionin virallinen lehti, 2016; Tietosuojavaltuutetun toimisto, ei päiväystä). Muutos on näkynyt käyttäjille selvimmin erilaisina lupapyyntöinä evästeisiin liittyen (Sanchez-Rola ym., 2019).

Sivuston ylläpitäjät voivat käyttää evästeitä, tässä tapauksessa seurantaevästeitä, esimerkiksi myyntiprosessin optimointiin. Niiden avulla on myös mahdollista toteuttaa esimerkiksi verkkokaupan ostoskori. (Kaspersky, ei päiväystä). Evästeet ovat internetissä pitkään käytetty tekniikka, jonka avulla on mahdollista saada selain ja palvelin muistamaan toisensa (Internet Engineering Task Force, 2011). Tämä itsessään vaarattomalta kuulostava toiminto ulkoistetaan kuitenkin useimmiten kolmannelle osapuolelle, jotka voivat sitten seurata käyttäjän liikkeitä erittäin tarkasti internetissä (Englehardt & Narayanan, 2016).

Käyttäjien seuranta tapahtuu internetissä usein. Sen tarkoituksena on kerätä palasia käyttäjän selaushistoriasta ja tehdä niiden tietojen perusteella jotain johtopäätöksiä. Yksittäisen sivuston tapauksessa käyttäjien seurannalla voidaan pyrkiä esimerkiksi mittaamaan automatisoidun myyntiprosessin toimivuutta ja tulosten perusteella tehostamaan sitä. Suuremmassa mittakaavassa käyttäjien seuranta voidaan käyttää myös käyttäjän mielenkiinnon kohteiden selvittämiseen, jotta hänelle voidaan näyttää kiinnostavampia mainoksia. (Urban ym., 2020). Tämä herättää kysymyksen, voisiko sivuston ylläpitäjä täyttää omat tarpeensa käyttäjien seurannasta vaarantamatta heidän tietosuojansa. Tämä työ on kuitenkin kirjallisuuskatsaus, joten lopulliseksi tutkimuskysymykseksi muotoutui ”Miten GDPR on vaikuttanut käyttäjien seurannan toteuttamiseen evästeillä?”

Käyttäjien seuranta on tutkittu jo ennen kuin GDPR nosti asian esille. Esimerkiksi Englehardt ja Narayanan (2016) osoittivat, että on olemassa pieni joukko yrityksiä, jotka kykenevät seuraamaan käyttäjien liikkeitä internetissä huomattavalla tarkkuudella. Varsinkin vuoden 2018 jälkeen on ilmestynyt huomattava määrä tutkimusta aiheen ympäriltä. Esimerkiksi erilaisten evästekyselyiden toimivuutta ovat tutkineet Utz ym. (2019).

GDPR:n myötä evästekyselyt ovat yleistyneet (Degeling ym., 2019). Se on internetsivuilla näytettävä kysely, jonka tarkoituksena on pyytää käyttäjältä suostumus evästeiden käyttämiseen (Kulyk ym., 2020). Terminä evästekysely on vähän harhaanjohtava, koska se tarkoittaa kaikenlaisia evästeiden käytöstä kertovia viestejä, myös niitä, jotka eivät ole suoranaisesti kyselyitä. Siksi tässä työssä käytetään termiä evästeilmoitus, kun tarkoitetaan evästekyselyä, jonka voi korkeintaan kuitata luetuksi.

Tehdystä kirjallisuuskatsauksesta voi olla hyötyä yrityksille esimerkiksi siten, että lisääntyneen tiedon avulla hyvä tietosuoja voitaisiin kokea hyödyllisenä työkaluna pakollisen pahan sijasta. Tämä tutkielma pohjautuu keväällä 2021 Johdatus tutkimustyöhön -kurssilla tehtyyn JTT-tutkielmaan (Hyytiälä, 2021).

Luvussa kaksi käsitellään tutkimusmenetelmää. Kolmannessa luvussa käsitellään aiempaa tutkimusta ja aiheen laajuuden vuoksi aiheen käsittely on jaettu kuuteen alilukuun. Neljännessä luvussa pohditaan aiempien tutkimusten keskeisiä teemoja. Viidennessä eli viimeisessä luvussa kootaan kaikki yhteen johtopäätösten muodossa sekä tuodaan esille mahdollisia jatkotutkimusaiheita.

2. Tutkimusmenetelmä

Tutkimusmenetelmäksi valittiin kirjallisuuskatsaus. Breretonin ym. (2007) esittämän kymmenen kohdan menetelmästä tässä tutkimuksessa käytettiin hieman kevennettyä versiota. Pääpaino on heidän menetelmänsä pääkohdissa, jotka ovat suunnittelu, toteutus ja raportointi. Nämä kolme vaihetta suoritettiin järjestyksessä.

Tutkimusongelma nivoutuu varsin tiukasti kahden termin ympärille, jotka ovat GDPR ja evästeet. Näistä termeistä on olemassa hieman erilaisia ja vähemmän käytettyjä variaatioita, joiden etsimiseen käytettiin Scopusin avainsanatyökalua.

Koska entuudestaan tiedossa oli jo kaksi vahvaa aiheeseen liittyvää termiä, aineistonkeruu aloitettiin yksinkertaisesti tekemällä Scopusissa otsikkoon, tiivistelmään ja avainsanoihin kohdistuva haku lausekkeella “gdpr and cookie”. Ensimmäisellä haulla löytyi 32 osumaa, joista lähes kaikki on kirjoitettu vuoden 2018 jälkeen.

Tätä hakutulosta käytettiin pohjamateriaalina Scopusin avainsanatyökalulle. Sen avulla löytyi muutama muu aiheeseen liittyvä termi, jotka olivat evästekysely, evästeilmoitus ja sähköisen viestinnän tietosuojaa-asetus.

Lopulliseksi hakulausekkeeksi muodostui “(gdpr or eprivacy) and (cookie or “cookie consent” or “cookie notice”)”. Scopusin otsikkoon, tiivistelmään ja avainsanoihin kohdistuvalla haulla löytyi yhteensä 39 osumaa. Näistäkin suurin osa on kirjoitettu vuoden 2018 jälkeen.

Tulosjoukosta rajattiin käytännöllisistä syistä pois muut kuin englanninkieliset artikkelit. Lisäksi joidenkin artikkeleiden kokotekstiversio ei ollut saatavilla, joten nekin jouduttiin rajaamaan pois.

Tulosten analysoinnissa kävi ilmi, että lopullinen hakulauseke kasvatti tulosjoukkoa vain seitsemällä osumalla. Näistä merkittävin osa on kirjoitettu ennen vuotta 2018. Tämä saattaa kertoa siitä, että terminä GDPR on niin vahva, että se mainitaan useimmissa vuoden 2018 jälkeen julkaistuissa aiheita käsittelevissä artikkeleissa. Toisaalta se on myös vielä niin uusi termi, että sitä käsitteleviä artikkeleita ei ole ehtinyt kertyä kovin paljon.

Lisäksi Scopusin avulla etsittiin tämän tulosjoukon lähdeluetteloista aiheeseen liittyviä muita artikkeleita. Sillä tavalla Scopusista löytyi yhteensä 490 tieteellistä artikkelia, joiden joukosta poimittiin käsin muutama artikkeli käytettäväksi lähteenä tässä kirjallisuuskatsauksessa.

Tiedonhakuun käytettiin pelkästään Scopusia, koska kaikki sieltä löytyvät artikkelit ovat vertaisarvioituja ja jokaista artikkelia ei tarvinnut tällöin arvioida erikseen. Tätä kirjallisuuskatsausta varten tarvittiin lähteiksi vähintään 20 empiiristä tutkimusta, jotka löytyivät tällä tavalla kohtuullisen helposti.

3. Tutkimustulokset

Kolmannen osapuolen evästeitä ja evästeitä yleensäkin on käytetty melko pitkään, sillä ainakin van Eijkin ym. (2012) tutkimuksen aikaan ne olivat hyvin yleisiä. Heidän mukaansa niihin yhdistettiin siihen aikaan usein yksilöiviä henkilötietoja esimerkiksi mainosten kohdentamiseksi.

Van Eijkin ym. (2012) tutkimuksen aikaan käytössä oli myös Flash-pohjaisia evästeitä, joiden olemassaolosta suurin osa käyttäjistä ei ollut tietoisia eikä siten osannut esimerkiksi poistaa niitä. Nykyään käyttäjiä seurataan muillakin kuin evästepohjaisilla menetelmillä, joihin lukeutuvat esimerkiksi selaimen sormenjäljen muodostaminen (Englehardt & Narayanan, 2016; Papadogiannakis ym., 2021).

3.1 Evästeistä kertominen

Vanha vuoden 2002 sähköisen viestinnän tietosuoja-asetus edellytti luvan kysymistä käyttäjältä evästeiden käytön osalta, mutta siitä huolimatta noin 50 % sivustoista ei kysynyt käyttäjältä lupaa evästeille van Eijkin ym. (2012) tutkimuksen mukaan. Osalle heidän tutkimukseensa osallistuneista yrityksistä oli epäselvää, mitkä tilanteet eivät lukeutuneet niihin lain määrittelemiin poikkeuksiin, joihin lupaa ei tarvinnut pyytää. Heidän mukaansa luvan pyytäminen saattoi kuitenkin siihen aikaan tarkoittaa samaa kuin palvelun yleisten ehtojen hyväksyminen.

Tämän lisäksi evästeiden käytöstä tuli kertoa käyttäjälle mutta van Eijkin ym. (2012) tutkimuksen mukaan erityisesti kolmannen osapuolen evästeiden osalta oli monin paikoin epäselvää, kuka niistä kertoo käyttäjälle. Fouad ym. (2020) havaitsivat tutkimuksessaan, että vain 13 % sivustoista kertoo erikseen kolmannen osapuolen evästeitä käyttäjille. Heidän mukaansa evästeiden tarkoitus kerrotaan selvästi vain 5 % sivustoista.

Degelingin ym. (2019) tutkimuksen mukaan evästeistä kertomisesta tuli hieman yleisempää vuonna 2018, kun GDPR astui voimaan. Heidän mukaansa evästeistä kerrottiin vähän yli 60 % sivustoista elokuussa 2018. Lähes samaan tulokseen pääsivät vuotta myöhemmin myös Bornschein ym. (2020).

Muista samaa asiaa tutkineista poiketen Hu ja Sastry (2019) tutkivat yleisimmin vierailtujen internetsivujen lisäksi myös tutkimushenkilöiden selaushistoriaa, johon lukeutui myös paljon harvemmin käytettäviä sivustoja. Heidän tutkimuksensa mukaan 45 % muistakin kuin vain isoimmista sivustoista ei kertonut käyttäjille evästeistä.

Uudemmissa tutkimuksissa havaittiin aiemmista tutkimuksista poiketen, että vain noin 45 % sivustoista kertoo evästeiden käytöstä (Kampanos & Shahandashti, 2021). Heidän mukaansa ero voi selittyä myös suuremmalla otannalla.

Samalla kun merkittävä osa sivustoista ei kerro evästeistä mitään, yli 90 % sivustoista käyttää kuitenkin evästeitä. Evästeitä käytetään usein jo ennen kuin käyttäjä on antanut siihen luvan. (Sanchez-Rola ym., 2019.) Myös Dabrowski ym. (2019) tulivat siihen tulokseen, että vähän yli 30 % sivustoista tallentaa evästeitä ennen luvan saamista.

Koska Eurooppa on ensimmäisten joukossa ryhtynyt parantamaan käyttäjien tietosuojaa lainsäädännön tasolla, on hyvin ymmärrettävää, että Hun ja Sastry (2019) tutkimuksen

mukaan eurooppalaisilla sivustoilla evästeiden käytöstä kerrottiin useammin kuin muualla maailmassa. Samaan tulokseen tulivat myös Sanchez-Rola ym. (2019).

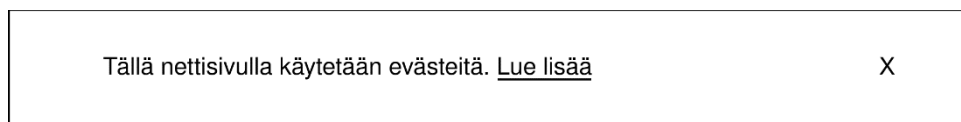
Vastaavasti Dabrowski ym. (2019) havaitsivat, että käyttäjän maantieteellinen sijainti vaikutti evästeiden käyttämiseen tai käyttämättä jättämiseen lähinnä suosituimman tuhannen sivuston joukossa. Heidän mukaansa ero saattaa selittyä sillä, että merkittävä osa suosituimmista sivustoista on keskittynyt ansaitsemaan mainostuloilla ja asiaan on panostettu siksi näillä sivustoilla muita enemmän.

3.2 Erilaiset evästekyselyt

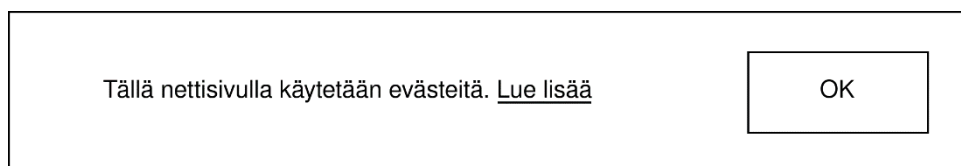
Useissa tutkimuksissa evästekyselyt jaetaan kategorioihin pääpiirteissään samalla tavalla. Esimerkiksi Kampanos ja Shahandashti (2021), Degeling ym. (2019), Hu ja Sastry (2019) ja Utz ym. (2019) jakoivat evästekyselyt eri toimintojen lukumäärän mukaan vaikkakin keskenään hieman eri tavalla. Lisäksi Bornschein ym. (2020) jakoivat evästekyselyt niiden koon mukaan ja Utz ym. (2019) sen mukaan, missä kohtaa näyttöä ne sijaitsivat.

Muista poiketen Kulyk ym. (2020) jakoivat evästekyselyt niiden sisältämän tekstisisällön mukaan. He tosin eivät havainneet evästekyselyn tekstillä olevan kovinkaan suurta vaikutusta mihinkään. Yksi potentiaalinen syy voi olla siinä, että ihmiset eivät oikeasti lue evästekyselyä (Kulyk ym., 2020), mikä sinällään vesittäisi koko kyselyn tarkoituksen.

Bornscheinin ym. (2020) tutkimuksesta 60 % evästekyselyistä on pieniä ja eivät sisällä aitoa mahdollisuutta kieltäytyä evästeistä. Vastaavasti Kampanos ja Shahandashti (2021) havaitsivat, että 91 % evästekyselyistä ei tarjoa kieltäytymismahdollisuutta. Muissa tutkimuksissa puolestaan havaittiin, että 60 %:lla (Soe ym., 2020) ja 50 %:lla (Mehrnezhad, 2020) sivustoista evästekyselyt sijaitsivat näytön alareunassa.



Kuva 1. Evästeilmoitus, jonka käyttäjä voi vain sulkea.



Kuva 2. Evästeilmoitus, jossa käyttäjä voi vain hyväksyä evästeiden käytön.

Kuvat 1 ja 2 esittävät näitä pieniä ja huomaamattomia evästeilmoituksia, joissa käyttäjällä ei ole aitoa mahdollisuutta kieltäytyä evästeistä. Käytännössä nämä kaksi evästekyselytyyppiä ovat ne, joita on puolet kaikista evästekyselyistä esimerkiksi Bornscheinin ym. (2020) tutkimuksen mukaan.

Tällä nettisivulla käytetään evästeitä. [Lue lisää](#)

Ei kiitos

OK

Kuva 3. Evästekysely, jossa käyttäjä voi myös kieltäytyä evästeistä.

Tällä nettisivulla käytetään evästeitä. [Lue lisää](#)

☒
Välttämättömät

☐
Muu tarkoitus A

☐
Muu tarkoitus B

☐
Muu tarkoitus C

Vain valitut

Salli kaikki

Kuva 4. Evästekysely, jossa käyttäjä voi valita haluamansa evästeet.

Kuvassa 3 on yksinkertainen evästekysely, jossa käyttäjällä on aito mahdollisuus kieltäytyä evästeistä. Lisäksi kuva 4 esittää vähän monimutkaisempaa evästekyselyä, jossa käyttäjä voi valita haluamansa evästeet. Tämän tyyppiset evästekyselyt ovat puolestaan varsin harvinaisia Bornscheinin ym. (2020) tutkimuksen mukaan.

Vaikka suurin osa evästekyselyistä onkin pieniä ja huomaamattomia, Nouwensin ym. (2020) tutkimuksen mukaan sillä ei kuitenkaan ole merkittävää vaikutusta aidon hyväksymisen ja kieltäytymisen keskinäiseen suhteeseen, mikäli siis niistä käytettäisiin sellaista versiota, jossa on myös kieltäytymismahdollisuus. Heidän tutkimuksessaan havaittiin, että helpommin ohitettavissa oleva evästekysely ohitetaan 3,6 kertaa todennäköisemmin kuin vaikeammin ohitettava, mikä luonnollisesti vaikuttaa saatujen hyväksyntöjen lukumäärään.

3.3 Evästeistä kieltäytyminen

Sinä missä lähes kaikilla sivustoilla käytetään evästeitä ja vain osassa sivustoista kerrotaan niistä käyttäjälle, Hu ja Sastry (2019) havaitsivat, että 35 % brittiläisistä sivustoista kertoi evästeistä käyttäjälle mutta ei antanut aitoa mahdollisuutta kieltäytyä niistä. Näihin yleisimmillä – eli pienillä ja huomaamattomilla – evästeilmoituksilla Utzin ym. (2019) tutkimuksen mukaan evästeiden käyttö hyväksytään painamalla ainoaa nappia 2–18 % todennäköisyydellä riippuen sen sijainnista näytöllä, kun taas se ohitetaan 65–98 % todennäköisyydellä.

Utzin ym. (2019) tutkimuksen mukaan vajaa 60 % sivustoista ohjaa käyttäjiä hyväksymään evästeet esimerkiksi hankaloittamalla niistä kieltäytymistä. Heidän tutkimuksensa mukaan hienovarasellakin ohjaamisella on havaittu olevan hyväksymistodennäköisyyttä parantava vaikutus, joskaan vaikutus ei ole kovin suuri. Myöhemmin Bauer ym. (2021) havaitsivat tällaisten toimien parantavan hyväksymistodennäköisyyttä jopa 17 %-yksikköä neutraaliin kontrolliversioon verrattuna.

Näiden lisäksi Sanchez-Rola ym. (2019) havaitsivat tutkimuksessaan käytössä olevan vielä muunkinlaisia evästeiden hyväksymiseen ohjaavia käyttöliittymäratkaisuja. Vaikka kaikkien erilaisten käyttäjiä ohjaavien toimenpiteiden vaikutusta ei ole vielä tutkittu, tutkimustulosten valossa on selvää, että käyttäjiä voi suostutella melko tehokkaasti ainakin joillakin keinoilla.

Samalla kun käyttäjiä ohjataan usein hyväksymään evästeet, aidon hylkäämismahdollisuuden tarjosi vain alle 5 % sivustoista (Sanchez-Rola ym., 2019). Hylkäämiselläkään ei aina ole kuitenkaan mitään vaikutusta eli evästeiden käyttö jatkuu joillakin sivustoilla senkin jälkeen (Matte ym., 2020).

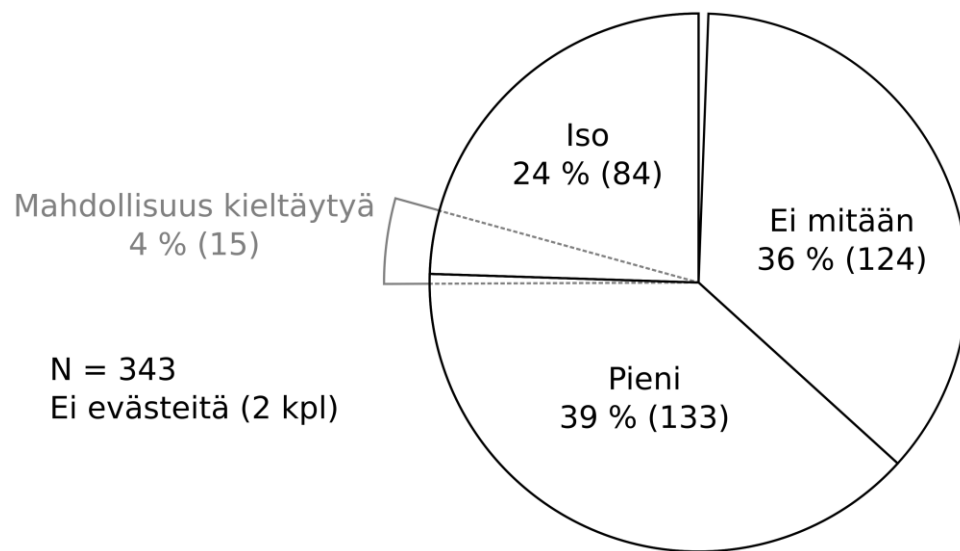
Myös muissa tutkimuksissa havaittiin, että 4 % (Bornschein ym., 2020), 5 % (Soe ym., 2020) ja 8 % (Kampanos & Shahandashti, 2021) sivustoista tarjosi aidon mahdollisuuden kieltäytyä evästeistä. Tämän tyyppisissä evästekyselyissä aito hyväksyntä saadaan 0–41 % todennäköisyydellä (Utz ym., 2019).

Kieltäytymisen on havaittu vaativan noin 50 % sen mahdollistavista sivustoista keskimäärin 10–12 napin painallusta, kun taas hyväksyminen onnistui kaikilla tutkituilla sivustoilla yhdellä napin painalluksella (Soe ym., 2020). Vastaavasti evästeiden asettamisen jälkeen noin 15 % sivustoista tarjosi mahdollisuuden muuttaa valintaa myöhemmin (Sanchez-Rola ym., 2019).

Utzin ym. (2019) mukaan evästekyselyn sijainnilla, vaihtoehtojen määrällä sekä näytön koolla vaikuttaisi olevan jonkinlaista vaikutusta hyväksymistodennäköisyyteen sekä yleensä ottaen evästekyselyyn vastaamiseen. Kuitenkin evästekysely ohitetaan heidän mukaansa 55–98 % todennäköisyydellä riippuen sen sijainnista näytöllä.

Evästekyselyyn vastaaminen vie käyttäjältä keskimäärin 4–8 sekuntia, kun taas 84 % käyttäjistä poistuu sivulta 10 sekunnin sisällä sinne saapumisesta (Utz ym., 2019). Eli tämä 84 % käyttäjistä ehti keskittyä sivuston varsinaiseen sisältöön 2–6 sekuntia ennen sivulta poistumista, mikäli evästekysely esti sivuston varsinaisen sisällön näyttämisen käyttäjälle. Tähän liittyen Kulykin ym. (2020) tutkimuksen mukaan saattaisi olla mahdollista, että evästekyselyn koolla olisi vaikutusta sivustolta poistumisen todennäköisyyteen.

Utzin ym. (2019) tutkimukseen osallistuneista noin 20 % käytti mainostenestovelluksia. Niistä edistyneimmissä saattaa olla nykyään toimintoja yleisimpien seurantaevästeiden estämiseen ja evästekyselyiden piilottamiseen. Niiden käyttäminen voisi siis nostaa evästekyselyn automaattista hylkäämis- tai ohittamistodennäköisyyttä.



Kuva 5. Erilaisten evästekyselyiden yleisyys (Borchein ym., 2020).

Kuva 5 esittää erilaisten evästekyselyiden yleisyyttä Borcheinin ym. (2020) tutkimuksen mukaan. Evästeitä käytetään 99 % sivustoista. Minkäänlaista evästekyselyä ei kuitenkaan näytetä 36 % sivustoista. Pienikokoinen evästekysely näytetään 39 % ja isokokoinen 24 % sivustoista. Näissäkin vain pieni osa tarjoaa mahdollisuuden kieltäytyä evästeistä. (Borcheinin ym., 2020).

3.4 Kolmannen osapuolen evästeet

Nyt kun olemme tarkastelleet evästeistä kertomista luvussa 4.2 ja niistä kieltäytymistä luvussa 4.3, on aika tarkastella hieman varsinaisen tietosuojauhan aiheuttavia evästeitä eli seurantaevästeitä. Seurantaevästeet ovat evästeitä, joiden avulla voidaan seurata käyttäjän liikkeitä sivustolla tai kolmannen osapuolen asettamien seurantaevästeiden tapauksessa monilla eri sivustoilla.

Vain reilu 10 % sivustoista käyttää omia seurantaevästeitä. Vastaavasti yli puolet on ulkoistanut sen jollekin tunnetulle kolmannelle osapuolelle. Loppuosaa ei saatu tunnistettua. (Sanchez-Rolan ym., 2019.) Uudemmissa tutkimuksissa Kampanos ja Shahandashti (2021) havaitsivat, että noin 68 % sivustoista käyttää kolmannen osapuolen evästeitä.

Seurantaevästeiden ulkoistamisessa on sellainen ongelma, että se keskittyy Englehardtin ja Narayananin (2016) tutkimuksen mukaan vain muutamalle isolle toimijalle, jotka ovat Google, Facebook, Twitter ja AdNexus. Näistä neljästä toimijasta jokaisen jalansija internetissä on heidän tutkimuksensa mukaan yli 10 %, Googlen jopa yli 60 %, joten niillä on kyky seurata ihmisten liikkeitä internetissä huomattavalla tarkkuudella.

GDPR:n käyttöönotto ei ole tuonut tähän merkittävää muutosta. Kolmansien osapuolien lukumäärässä ei tapahtunut merkittävää muutosta mutta joitakin kolmansia osapuolia tippui pois ja tilalle tuli uusia (Sørensen & Kosta, 2019). Kuitenkin isot toimijat dominoivat markkinoita edelleenkin (Sørensen & Kosta, 2019; Urban ym., 2020). Näiden isojen toimijoiden joukossa seurantaevästeiden jakaminen toisilleen on myös yleistä (Englehardt & Narayanan, 2016).

Kolmannen osapuolen evästeiden käytössä on potentiaalisena ongelmana se, että sivusto ei voi poistaa kolmannen osapuolen asettamia evästeitä itse, vaan kyseisen evästeen asettanut kolmas osapuoli joutuu tekemään sen (Degeling ym., 2019). Eli evästeen asettavan kolmannen osapuolen täytyisi tarjota sivustolle toiminto, jolla evästeen voi poistaa, mikäli sivusto tarjoaa käyttäjälle mahdollisuuden perua antamansa suostumuksen jonkinlaisen sivustolle upotetun käyttöliittymän kautta.

Sørensenin ja Kostan (2019) tutkimuksen mukaan sivustoilla käytetyistä kolmansista osapuolista selkeästi suurin yksittäinen kategoria on keskittynyt mainontaan. Näistä mainoksiin keskittyneistä toimijoista moni tarjosi käyttäjälle seurannasta kieltäytymisen jo ennen GDPR:ää (Sakamoto & Matsunaga, 2019).

Kieltäytymisestä huolimatta noin joka toisessa tapauksessa seuranta kuitenkin jatkui eikä tilanne ole muuttunut olennaisesti GDPR:n voimaantulon jälkeen (Sakamoto & Matsunaga, 2019). Myös Matte ym. (2020) havaitsivat valmiskyselyjä tutkiessaan, että evästeistä kieltäytymisen ja sivun päivittämisen jälkeen lähes aina isot kolmannet osapuolet olivat kuitenkin taas paikalla.

3.5 Valmiskyselyt

Siinä missä seurantaevästeet on usein ulkoistettu kolmannelle osapuolelle, myös evästekyselyn toteuttamisen on ulkoistanut kolmannelle osapuolelle 57 % sivustoista, joissa evästekysely on yleensä ottaen toteutettu. Edes nämä kolmannen osapuolen tarjoamat valmiskyselyt eivät takaa automaattista lain kirjaimen noudattamista, sillä valmiskyselyä käyttävistä sivustoista 11 % noudatti lain vaatimaa minimiä. (Nouwens ym., 2020).

Selkeästi yleisin virhe oli esivalittu rasti, jollaisia löytyi 56 % tutkituista sivustoista (Nouwens ym., 2020). Esivalittu rasti todettiin lain vastaiseksi Euroopan unionin tuomioistuimen (2019) tuomiossa, joka liittyi Planet49-tapaukseen.

Tällä nettisivulla käytetään evästeitä. [Lue lisää](#)

<input checked="" type="checkbox"/> Välttämättömät	<input type="checkbox"/> Mielitymykset
<input checked="" type="checkbox"/> Tilastot	<input checked="" type="checkbox"/> Markkinointi
<div style="border: 1px solid black; padding: 5px; width: 100%;">Vain valitut</div>	<div style="border: 1px solid black; padding: 5px; width: 100%;">Salli kaikki</div>

Kuva 6. Evästekysely, jossa on esivalittuja rasteja.

Kuva 6 esittää kaikkein tyypillisintä lain vastaista evästekyselyä, jossa käyttäjällä on aito mahdollisuus kieltäytyä evästeistä, mutta jossa joitakin rasteja on esivalittu.

Edellisen lisäksi myös Matte ym. (2020) tutkivat tietyn tyyppisiä valmiskyselyitä. Heidän tutkimuksensa mukaan evästekyselyjä käyttävistä sivuista 54 % ei täyttänyt lain vaatimaa minimiä ja vastaavasti yleisin rikkomus oli esivalittu rasti, jota löytyi joka toisesta tapauksesta.

3.6 Lopuksi

Useissa tutkimuksissa on tutkittu erilaisia evästekyselyitä ja niiden toimivuutta erityisesti evästeiden hyväksyntää silmällä pitäen. Utz ym. (2019) tutkivat myös sitä, miten suuri osa sivustolla vierailemiseen käytetystä ajasta menee evästekyselyn hyväksymiseen tai hylkäämiseen.

Utzin ym. (2019) tutkimuksen lisäksi evästekyselyiden seurauksia tarkastelevan tutkimuksen olivat tehneet Bornschein ym. (2020). He havaitsivat tutkimuksessaan, että kaikenlaiset evästekyselyt nostavat käyttäjän kokemaa riskiä ja riski puolestaan laskee ostohalua.

Vastaavasti käyttäjän kokema hallinnan tunne laskee, mikäli näytetään evästeilmoitus, jossa ei voi kieltäytyä evästeistä (Bornschein ym., 2020). Tämän lisäksi evästeiden aidolla hyväksymisellä havaittiin myös olevan positiivinen vaikutus hinnankorotuksen hyväksymisessä esimerkiksi lentoyhtiöiden käyttämässä dynaamisen hinnoittelun mallissa (Schmidt ym., 2020).

Nämä tulokset näyttävät antavan tukea Strycharzin ym. (2021) hypoteesille siitä, että jos evästeiden käyttötarkoitus kerrotaan avoimesti, se laskee käyttäjän kokemaa riskin tunnetta ja lisää hallinnan tunnetta, joilla taas on vaikutusta siihen, että käyttäjä hyväksyy evästeiden käytön todennäköisemmin. Moni kokee evästekyselyt myös häiritsevänä tai ärsyttävänä mutta samalla ihmiset ovat alkaneet kuitenkin jo tottua niihin (Kulyk ym., 2020). Eli vaikka aihe jakaakin mielipiteitä, aihe ei välttämättä herätä enää samalla tavalla tunteita kuin pari vuotta sitten.

4. Pohdinta

Tässä luvussa esitetään tutkimukseen pohjautuvia huomioita omissa alaluvuissaan.

4.1 Lain kirjaimen noudattaminen

GDPR astui voimaan siten, että sen vaatimukset otettiin huomioon merkittäväällä osalla internetsivuista kevään 2018 aikana. Samaan aikaan aiheen yhteiskunnallinen merkitys kasvoi huomattavasti ja siten myös aiheesta löytyy tieteellistä tutkimusta lähinnä vuodesta 2019 lähtien.

Suurin osa tähänastisesta tutkimuksesta keskittyy vahvasti erilaisiin evästekyselyihin sekä siihen, miten monella sivustolla lain vaatima minimi täyttyi. Esimerkiksi Degelingin ym. (2019) ja Bornscheinin ym. (2020) tutkimuksissa havaittiin, että noin puolet sivustoista ei kerro evästeistä käyttäjille, vaikka lähes kaikilla sivustoilla käytetään evästeitä.

Jäljelle jäävistä sivustoista puolet kertoo käyttäjälle evästeistä evästeilmoituksella, mutta ei anna käyttäjälle aitoa mahdollisuutta kieltäytyä niistä (Bornschein ym., 2020), ja evästekyselyt muutenkin helposti ohitettavissa sijaintinsa takia (Mehrnezhad, 2020; Soe ym., 2020). Loput sivustot käyttävät jotakin sellaista evästekyselyä, jossa käyttäjällä on mahdollisuus kieltäytyä evästeistä (Bornschein ym., 2020).

Vaikka neljännes kaikista sivustoista tarjoaakin käyttäjälle näennäisen mahdollisuuden kieltäytyä evästeistä, useissa tutkimuksissa havaittiin, että aidon kieltäytymismahdollisuuden tarjosi noin 5–8 % sivustoista (Bornschein ym., 2020; Kampanos & Shahandashti, 2021; Sanchez-Rola ym., 2019; Soe ym., 2020) mutta kieltäytymisellä ei kuitenkaan havaittu olevan vaikutusta mihinkään (Sanchez-Rola ym., 2019). Eli evästeiden käyttö jatkuu kieltäytymisen jälkeenkin.

Lisäksi esimerkiksi Utzin ym. (2019) tutkimuksessa kävi ilmi, että reilu puolet evästekyselyn sisältävistä sivustoista hyödyntää käyttöliittymäratkaisuja, jotka ohjaavat käyttäjää hyväksymään evästeet. Vastaavasti reilu puolet evästekyselyistä on toteutettu jonkin kolmannen osapuolen tarjoaman valmiskyselyn avulla (Nouwens ym., 2020).

Nouwens ym. (2020) ja Matte ym. (2020) tutkivat valmiskyselyitä käyttäviä sivustoja. Heidän tutkimuksissaan lopputulokset poikkeavat toisistaan, sillä Nouwensin ym. (2020) tutkimuksen mukaan noin 10 % tutkituista sivustoista täytti lain vaatiman minimin, kun taas Matten ym. (2020) tutkimuksen mukaan vajaa puolet ylsi siihen.

Eroavaisuudet saattavat selittyä ainakin osittain otantajoukolla, sillä Matten ym. (2020) tutkimuksessa tutkittiin vain tietyn tyyppisiä valmiskyselyitä käyttäviä sivustoja. Koska aihe on vielä tieteellisessä mielessä melko tuore, aiheeseen liittyvät määritelmät eivät ole vielä välttämättä vakiintuneet niin, että rajatapauksissa tutkijan näkökanta on saattanut vaikuttaa siihen, mikä määritellään lain vastaiseksi ja mikä ei.

Vaikka monet lukemat vaikuttavatkin olevan keskenään ristiriidassa, kaikista tutkimuksista käy selkeästi ilmi, että moni sivusto saa tutkijoilta kritiikkiä lain kirjaimen noudattamisesta.

4.2 Kolmansien osapuolien harjoittama seuranta

Kolmansien osapuolien evästeiden käytössä ei havaittu tapahtuneen merkittäviä muutoksia ennen vuotta 2018 ja sen jälkeen (Sørensen & Kosta, 2019). Seurantaevästeet ulkoistetaan lähes aina kolmannelle osapuolelle (Sanchez-Rola ym., 2019). Näistä kolmansista osapuolista löytyy todella isoja toimijoita, joiden markkinaosuus on niin iso, että ne pystyvät seuraamaan käyttäjien liikkeitä internetissä huomattavalla tarkkuudella (Englehardt & Narayanan, 2016).

Kolmannen osapuolen evästeissä on havaittu olevan samoja haasteita lain kirjaimen noudattamisessa kuin evästeissä yleensäkin (van Eijk ym., 2012; Sakamoto & Matsunaga, 2019). Esimerkiksi Matten ym. (2020) tutkimuksen mukaan kolmannen osapuolen evästeistä kieltäytyminen ei lopeta seurantaa.

4.3 Evästekyselyiden käytön vaikutukset

Lain kirjaimen noudattamisen lisäksi tutkimusta on viime aikoina alettu tekemään myös evästeiden käytön vaikutuksista eri asioihin. Esimerkiksi Bornschein ym. (2020) havaitsivat, että kaikenlaiset evästekyselyt lisäävät käyttäjän kokemaa riskiä ja riski puolestaan vähentää ostohaluja.

Vastaavasti Utz ym. (2019) tutkivat sitä, miten kauan käyttäjältä kestää reagoida evästekyselyyn suhteessa sivustolla vietettyyn aikaan. Heidän tutkimuksensa mukaan monien käyttäjien sivustolla käyttämästä 10 sekunnista jopa yli puolet menee evästekyselyyn vastaamiseen.

Tähän kannattaa yhdistää vielä se, että yleisimmin käytetyillä evästekyselyillä hyväksyntä saadaan vain muutaman prosentin todennäköisyydellä, kun taas se ohitetaan yli kahden kolmasosan todennäköisyydellä (Utz ym., 2019).

4.4 Käyttäjien seurannan tulevaisuus

Suurin osa tutkimuksista keskittyi internetin suosituimpiin sivustoihin ja niilläkin vain etusivuihin. Vekarian ym. (2021) tutkimuksen mukaan ainakin intialaisilla uutissivustoilla käyttäjien seurannan määrä vaihtelee riippuen siitä, millä sivuston yksittäisellä sivulla käyttäjä vierailee. Tämän perusteella herää kysymys, tapahtuuko tätä myös laajemmassa mittakaavassa ja mikä vaikutus sillä on käyttäjien seurantaan kokonaisuudessa.

GDPR:n jälkeen myös muualla maailmassa on syntynyt vastaavan tyyppisiä tietosuojalakeja. Esimerkkeinä mainittakoon California Consumer Privacy Act (Kalifornia, USA), Lei Geral de Proteção de Dados Pessoais (Brasília) ja Protection of Personal Information Act (Etelä-Afrikka). Käyttäjien seurannan osalta evästeillä tapahtuva seuranta on saanut julkisuudessa paljon huomiota ja muut menetelmät ovat jääneet sen varjoon.

Käyttäjien seuranta internetissä pohjautuu nykypäivänä lähinnä muutamaan tekniikkaan (Englehardt & Narayanan, 2016; Papadogiannakis ym., 2021). Nämä tekniikat edellyttävät luonnollisesti sitä, että ne toimivat yleisimmissä selaimissa riittävän hyvin. Competition and Markets Authority (2020) arvioi raportissaan, että kaikkein suurin

vaikutus käyttäjien seurantaan on selainten kehittäjien tekemillä päätöksillä, ei niinkään eri maiden tietosuojalakeilla tai tuomioistuinten päätöksillä, vaikka niidenkään vaikutusta ei voi väheksyä.

Jotkut selaimet ovat jo tähänkin asti estäneet kolmannen osapuolen evästeiden toimimisen tavalla, joka tekee niistä hankalasti hyödynnettävän menetelmän käyttäjien seurannassa. Esimerkkinä mainittakoon Firefox ja Safari. Kolmannen osapuolen evästeiden aika näyttäisi olevan kohta ohi, sillä myös Google on lanseerannut The Privacy Sandbox -hankkeen, jonka tarkoituksena on muutaman vuoden kuluessa estää Chromesta kolmannen osapuolen evästeet samoin kuin esimerkiksi selaimen sormenjäljen muodostaminen (Schuh, 2019).

Samassa yhteydessä Google on luomassa menetelmän, jonka nimi on Federated Learning of Cohorts, eli FLoC. Ainakaan heidän mukaansa se ei vaaranna käyttäjän tietosuojaa (Web Platform Incubator Community Group, 2021). Myös Competition and Markets Authority (2020) pitää tätä todennäköisenä menetelmänä käyttäjien seurannalle tulevaisuudessa.

On mahdollista, että kaikki selaimet eivät kuitenkaan toteuttaisi FLoCia tai sitä ei voitaisi ottaa käyttöön jossakin päin maailmaa. Firefoxin ja Safarin lisäksi myös Chrome on estämässä kolmannen osapuolen evästeiden käytön muutaman vuoden sisällä (Goel, 2021). Tämä voi johtaa siihen, että nykyisten menetelmien tehokkuuden laskiessa tilalle syntyy myös muita menetelmiä, jotka on suunniteltu toimimaan esimerkiksi jossakin tietyssä maassa tai tietyllä selaimella.

Seurantamenetelmien pirstaloitumisen voi olettaa tuovan mukanaan yllätyksiä. Esimerkiksi Pathak ja Musku (2020) tutkivat mainosten kohdentamiseen soveltuvaa kontekstipohjaista menetelmää, joka ei edellytä henkilötietojen käsittelyä ollenkaan. Heidän tuloksensa olivat sen verran lupaavia, että aihetta kannattaisi tutkia vielä lisää. Riittäväällä tutkimuksella siitä voisi saada kilpailukykyisen menetelmän muiden rinnalle.

5. Johtopäätökset

Ensimmäisissä GDPR:ää ja evästeitä käsittelevissä tutkimuksissa pääpaino vaikuttaisi olevan pääsääntöisesti lain kirjaimen noudattamisessa. Esimerkiksi Nouwensin ym. (2020) tutkimuksessa havaittiin, että lain edellyttämä minimi täyttyi vain melko harvalla sivustolla. Tutkimusten valossa näyttäisi siltä, että suurimmalla osalla sivustoista lain noudattaminen on nähty lähinnä pakollisena pahana.

Aivan uusimmissa artikkeleissa tutkimuksen suunta on mahdollisesti kääntymässä tilanteeseen sopeutumisesta tilanteesta hyötymiseen. Esimerkiksi Schmidt ym. (2020) havaitsivat, että käyttäjän vastauksesta evästekyselyyn tai vastaamatta jättämisestä voidaan tehdä päätelmiä, joita voidaan hyödyntää myöhemmin myyntiprosessissa.

Koska aihealue on vielä melko tuore, myös uusimmista tutkimuksista löytyi mielenkiintoisia jatkotutkimusaiheita. Esimerkiksi Bornschein ym. (2020) nostivat esiin tutkimuskysymyksen, miten evästekyselyt vaikuttavat käyttäjien käyttäytymiseen ja lopulta ostokäyttäytymiseen eikä pelkästään ostohaluun, jota heidän tutkimuksessaan tutkittiin.

GDPR:n lyhyestä historiasta ja uusista teknologioista johtuen aiheita ei ole tutkittu vielä loppuun ja sitä voi tutkia monin eri tavoin. Useat empiiriset tutkimukset oli toteutettu rinnakkain toisistaan riippumatta ja niissä oli saatu jonkin verran toisistaan poikkeavia tuloksia, joten tulevaisuudessa voisi olla hyödyllistä tehdä yhteenveto tähänastisista tutkimustuloksista käsitteellisteoreettisen tutkimuksen muodossa.

Monissa tutkimuksissa oli kerätty mittavia määriä numeraalista aineistoa ja ainakin osa näistä aineistoista on vapaasti saatavilla internetissä. Suurin osa tutkimuksista perustui myös Alexa.com-palvelun listaukseen suosituimmista internetsivuista, joten aineistoissa on todennäköisesti paljon dataa samoista internetsivuista eri aikaväleiltä.

Jatkotutkimusta ajatellen näitä aineistoja voisi siksi olla järkevää yhdistellä ja tehdä sen pohjalta kattavampaa tutkimusta pidemmältä aikaväliltä. Tutkimusta ei tosin kannata välttämättä rajoittaa vain määrälliseen tutkimukseen, koska eri tutkimusmenetelmien yhdistämisestä on havaittu olevan hyötyä tutkimuksen tekemisessä (Kaplan ym., 1988).

Lähdeluettelo

- Bauer, J., Bergström, R. & Foss-Madsen, R. (2021). Are you sure, you want a cookie? – The effects of choice architecture on users' decisions about sharing private online data. *Computers in Human Behavior*, 120. <https://doi.org/10.1016/j.chb.2021.106729>.
- Bornschein, R., Schmidt, L. & Maier, E. (2020). The effect of consumers' perceived power and risk in digital information privacy: The example of cookie notices. *Journal of Public Policy and Marketing*, 39(2), 135–154. <https://doi.org/10.1177/0743915620902143>
- Brereton, P., Kitchenham, B., Budgen, D., Turner, M. & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, 80(4), 571–583. <https://doi.org/10.1016/j.jss.2006.07.009>
- Competition and Markets Authority. (1.7.2021). Online platforms and digital advertising, market study, final report, liite M. (s. 140). <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>
- Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G. & Weippl, E. (2019). Measuring Cookies and Web Privacy in a Post-GDPR World. Teoksessa D. Choffnes & M. Barcellos (toim.), *Lecture Notes in Computer Science: Vol 11419. Passive and Active Measurement* (s. 213–227). Springer. https://doi.org/10.1007/978-3-030-15986-3_17
- Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. & Holz, T. (24. – 27.2.2019). *We value your Privacy ... Now take some cookies: Measuring the GDPR's impact on web privacy* [Konferenssipaperi]. Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA. <https://doi.org/10.14722/ndss.2019.23378>
- Englehardt, S. & Narayanan, A. (2016). Online tracking: A 1-million-site measurement and analysis. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1388–1401. <https://doi.org/10.1145/2976749.2978313>
- Euroopan unionin virallinen lehti L 119, 4.5.2016, s. 1–88.
- Euroopan unionin tuomioistuin. (1.10.2019). *Tuomio asiassa C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV vastaan Planet49 GmbH* (EU:C:2019:801). Lainattu 3.3.2020, saatavilla:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=FI&mode=req&dir=&occ=first&part=1&cid=1447493>

Fouad, I., Santos, C., Al Kassar, F., Bielova, N. & Calzavara, S. (2020). On compliance of cookie purposes with the purpose specification principle. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 326–333.
<https://doi.org/10.1109/EuroSPW51379.2020.00051>

Goel, V. (24.6.2021). An updated timeline for Privacy Sandbox milestones [blogikirjoitus]. *The Keyword*. <https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/>

Hu, X. & Sastry, N. (2019). Characterising third party cookie usage in the EU after GDPR. *Proceedings of the 10th ACM Conference on Web Science*, 137–141.
<https://doi.org/10.1145/3292522.3326039>

Hyttiälä, J. (2021). *GDPR:n vaikutukset käyttäjien seurannan toteuttamiseen evästeillä* [julkaisematon JTT-tutkielma]. Oulun yliopisto.

Internet Engineering Task Force. (2011). *HTTP State Management Mechanism* (RFC 6265). <https://doi.org/10.17487/RFC6265>

Kampanos, G. & Shahandashti, S. (2021). Accept All: The Landscape of Cookie Banners in Greece and the UK. Teoksessa A. Jøsang, L. Futcher & J. Hagen (toim.), *IFIP Advances in Information and Communication Technology: Vol 625. ICT Systems Security and Privacy Protection* (s. 213–227). Springer.
https://doi.org/10.1007/978-3-030-78120-0_14

Kaspersky. (julkaisuaika tuntematon). *What are Cookies?* Haettu 22.10.2021 osoitteesta <https://www.kaspersky.com/resource-center/definitions/cookies>

Kaplan, B. & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *MIS quarterly*, 12(4), 571–586.
<https://doi.org/10.2307/249133>

Kulyk, O., Gerber, N., Hilt, A., & Volkamer, M. (2020). Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity*, 6(1).
<https://doi.org/10.1093/cybsec/tyaa022>

Matte, C., Bielova, N. & Santos, C. (2020). Do cookie banners respect my choice? Measuring legal compliance of banners from IAB Europe's transparency and consent framework. *2020 IEEE Symposium on Security and Privacy (SP)*, 791–809.
<https://doi.org/10.1109/SP40000.2020.00076>

- Mehrnezhad, M. (2020). A cross-platform evaluation of privacy notices and tracking practices. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 97–106. <https://doi.org/10.1109/EuroSPW51379.2020.00023>
- Nouwens, M., Liccardi, I., Veale, M., Karger, D. & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3313831.3376321>
- Papadogiannakis, E., Papadopoulos, P., Kourtellis, N., & Markatos, E. (2021). User tracking in the post-cookie era: How websites bypass GDPR consent to track users. *Proceedings of the Web Conference 2021*, 2130–2141. <https://doi.org/10.1145/3442381.3450056>
- Pathak, M., & Musku, U. (2020). Dynamic bidding with contextual bid decision trees in digital advertisement. Teoksessa M. Singh, K. Gupta, V. Tyagi, J. Flusser, T. Ören & G. Valentino (toim.), *Communications in Computer and Information Science: Vol 1244. Advances in Computing and Data Sciences* (s. 463–473). Springer. https://doi.org/10.1007/978-981-15-6634-9_42
- Sakamoto, T. & Matsunaga, M. (2019). After GDPR, still tracking or not? Understanding opt-out states for online behavioral advertising. *2019 IEEE Security and Privacy Workshops (SPW)*, 92–99. <https://doi.org/10.1109/SPW.2019.00027>
- Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P. & Santos, I. (2019). Can I opt out yet? GDPR and the global illusion of cookie control. *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 340–351. <https://doi.org/10.1145/3321705.3329806>
- Schmidt, L., Bornschein, R. & Maier, E. (2020). The effect of privacy choice in cookie notices on consumers' perceived fairness of frequent price changes. *Psychology and Marketing*, 37(9), 1263–1276. <https://doi.org/10.1002/mar.21356>
- Schuh, J. (22.8.2019). Building a more private web [blogikirjoitus]. *The Keyword*. <https://blog.google/products/chrome/building-a-more-private-web/>
- Soe, T. H., Nordberg, O. E., Guribye, F. & Slavkovik, M. (2020). Circumvention by design - Dark patterns in cookie consent for online news outlets. *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, artikkeli 19. <https://doi.org/10.1145/3419249.3420132>
- Sørensen, J. & Kosta, S. (2019). Before and after GDPR: The changes in third party presence at public and private European websites. *The World Wide Web Conference*, 1590–1600. <https://doi.org/10.1145/3308558.3313524>

- Strycharz, J., Smit, E., Helberger, N., & van Noort, G. (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior*, 120, artikkeli 106750. <https://doi.org/10.1016/j.chb.2021.106750>
- Tietosuojavaltuutetun toimisto. (julkaisuaika tuntematon). *Usein kysyttyä EU:n tietosuojasetuksesta*. Haettu 5.10.2021 osoitteesta <https://tietosuoja.fi/gdpr>
- Urban, T., Tatang, D., Degeling, M., Holz, T. & Pohlmann, N. (2020). Measuring the impact of the GDPR on data sharing in ad networks. *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 222–235. <https://doi.org/10.1145/3320269.3372194>
- Utz, C., Degeling, M., Fahl, S., Schaub, F. & Holz, T. (2019). (Un)informed consent: studying GDPR consent notices in the field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–990. <https://doi.org/10.1145/3319535.3354212>
- van Eijk, N., Helberger, N., Kool, L., van der Plas, A. & van der Sloot, B. (2012). Online tracking: Questioning the power of informed consent. *Info*, 14(5), 57–73. <https://doi.org/10.1108/14636691211256304>
- Vekaria, Y., Agarwal, V., Agarwal, P., Mahapatra, S., Balan Muthiah, S., Sastry, N. & Kourtellis, N. (2021). Differential Tracking Across Topical Webpages of Indian News Media. *13th ACM Web Science Conference 2021*, 299–308. <https://doi.org/10.1145/3447535.3462497>
- Web Platform Incubator Community Group. (22.7.2021). *Federated Learning of Cohorts*. Haettu 10.10.2021 osoitteesta <https://wic.github.io/floc/>